

RECEIVED

JUN 05 2020

CONSUMER PROTECTION

BakerHostetler

Baker&Hostetler LLP

Key Tower  
127 Public Square, Suite 2000  
Cleveland, OH 44114-1214

T 216.621.0200  
F 216.696.0740  
www.bakerlaw.com

William H. Berglund  
direct dial: 216.861.7416  
wberglund@bakerlaw.com

June 3, 2020

**VIA OVERNIGHT MAIL**

Attorney General Gordon MacDonald  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

*Re: Incident Notification*

Dear Attorney General MacDonald:

We are writing on behalf of our client, Fishing Partnership Support Services (“Fishing”), to notify you of a security incident involving five New Hampshire residents. Fishing is a non-profit organization that provides support services to New England fishermen and their families.<sup>1</sup>

Fishing recently conducted an investigation into suspicious activity originating from a small number of Fishing employees’ email accounts. As soon as Fishing became aware of the activity, it immediately took measures to secure the email accounts, contacted law enforcement, and launched an internal investigation. A cybersecurity firm was engaged to assist in a forensic analysis of this incident. The investigation determined that an unauthorized person accessed three Fishing employees’ email accounts at various dates between January 13, 2020 and February 3, 2020. The investigation did not determine whether any specific emails or attachments were viewed by the unauthorized person; however, Fishing was not able to rule out that possibility for any of the emails or attachments in the accounts. Fishing searched the emails and attachments that could have been viewed to identify personal information that may have been accessible to the unauthorized person. Information pertaining to a total of five New Hampshire residents was identified on April 9, 2020. The information varied by individual; however, it included the

---

<sup>1</sup> This notice does not waive Fishing’s objection that New Hampshire lacks personal jurisdiction over it related to any claims that may arise from this incident.

June 3, 2020

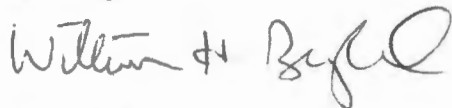
Page 2

individual's name in addition to one or more of the following data elements: Social Security number, driver's license number; and financial account number.

Beginning on June 3, 2020, Fishing will notify the New Hampshire residents in substantially the same form as the enclosed letters via United States Postal Service First Class Mail in accordance with N.H. Rev. Stat. Ann. § 359-C:20. Fishing is offering the New Hampshire individuals a complimentary, one-year membership to credit monitoring, fraud consultation, and identity theft restoration services through Kroll. Fishing is recommending that individuals remain vigilant to the possibility of fraud by reviewing their account statements for unauthorized activity. Fishing has also established a dedicated call center where all individuals may obtain more information regarding the incident.

To help prevent a similar incident from occurring in the future, Fishing is taking steps to enhance its existing security protocols and re-educating its staff for awareness on these types of incidents.

Sincerely,

A handwritten signature in black ink, appearing to read "William H. Berglund". The signature is fluid and cursive, with a large, stylized "W" and "B".

William H. Berglund  
Counsel

Enclosure

# FISHING PARTNERSHIP



S U P P O R T S E R V I C E S

<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

At Fishing Partnership Support Services ("Fishing"), we understand the importance of protecting and securing the personal information that we maintain. I am writing to inform you of an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

We recently conducted an investigation into suspicious activity originating from a small number of Fishing employees' email accounts. As soon as we became aware of the activity, we immediately took measures to secure the email accounts and launched an internal investigation. A cybersecurity firm was engaged to assist in a forensic analysis of this incident. The investigation determined that an unauthorized person accessed certain Fishing employees' email accounts at various dates between January 13, 2020 and February 3, 2020.

The investigation did not determine whether any specific emails or attachments were viewed by the unauthorized person; however, we were not able to rule out that possibility. We searched the emails and attachments that could have been viewed to identify individuals whose information may have been accessible to the unauthorized person. On April 9, 2020, we determined that an email or attachment in the accounts contained your <<b2b\_text\_1 (Impacted Data)>>.

We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. As an added precaution, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until **August 10, 2020** to activate your identity monitoring services.

Membership Number: <<Member ID>>

For more information on safeguarding your identity and your complimentary one-year membership, please see the additional information provided in this letter.

Your confidence and trust are important to us, and we sincerely regret any concern or inconvenience this incident may cause. To further protect personal information, we are taking steps to enhance our existing security protocols and re-educating our staff for awareness on these types of incidents. If you have any questions, please call 1-844-963-2714, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

A handwritten signature in black ink, appearing to be 'JJB'.

J.J. Bartlett  
President

## **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You've been provided with access to the following services<sup>1</sup> from Kroll:

### **Triple Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

If your health insurance or medical information was involved, it is also advisable to review the billing statements you receive from your health insurer or healthcare provider. If you see charges for services you did not receive, please contact the insurer or provider immediately.

### **Fraud Alerts and Credit or Security Freezes:**

**Fraud Alerts:** There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

**Credit or Security Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

**Additional information for residents of the following states:**

**New York:** You may contact and obtain information from these state agencies:

*New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and*

*New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>*